WISCONSIN DEPARTMENT OF CHILDREN AND FAMILIES
Division of Family and Economic Security
Bureau of Child Support

CHILD SUPPORT BULLETIN
No.: 12-08
Date: 06/22/2012

To: Child Support Directors
Child Support Supervisors or Lead Workers
Child Support Attorneys

From: Director
Bureau of Child Support

Subject: Federal Tax Information and IRS Security Measures

This Bulletin supersedes and obsoletes CSB 09-28R2

Purpose
This bulletin informs child support agencies of the requirements for ensuring the confidentiality of federal tax information (FTI) obtained from the Internal Revenue Service (IRS). These instructions have been updated based on the 2012 IRS Onsite Safeguard Review and the resulting findings and recommendations. The bulletin also includes a review of the bureau's plan to monitor local agency compliance with these requirements.

Background
The IRS is required by federal law to ensure that agencies with access to federal tax information follow stringent rules to ensure the confidentiality of personal tax information. You can find these requirements in IRS Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies.*

Policy
The IRS defines federal tax information (which is subject to safeguarding requirements) as any tax return-derived information received ***from the IRS***. All information that we receive from the IRS is subject to the safeguarding requirements. The IRS information in KIDS includes federal tax refund intercept-related information, IRS addresses, and IRS names.
Note: Tax forms provided to the CSA by a participant in the case are *not* considered federal tax information and are *not* subject to the IRS safeguarding requirements. They are, however, subject to the confidentiality requirements that apply in general to the child support program.
The definition of Federal Tax Information also includes any FTI that we receive from another state, e.g., a CSENet transaction or paper transmittal that informs us of a federal tax intercept collection made by the other state.

> ***Best Practice Tip:*** If you receive a paper transmittal from another state notifying you of a federal tax offset they applied to your case, make the appropriate adjustment to the account balance with a note stating that the adjustment was based on a collection processed in the other state. Create an event stating the same thing, and shred the transmittal. You must log the receipt and disposal of the transmittal.

Permitted Disclosure
The NCP (the taxpayer) is entitled to see his or her own tax information; and it is our position that the child support program cannot withhold case information from the CP that directly affects his or her account, including information about federal tax intercept collections.

IRS Safeguarding Requirements
Child support agencies that use IRS information must comply with IRS safeguarding requirements, including:

- Tracking and Disposal Requirements - Maintain a system of records and a log of activity of each printed IRS record, and properly dispose of IRS information;
- Secure Storage - Maintain secure storage of IRS information; provide minimum protection standards, identified as two barriers;
- Restricted Access - Restrict access to those staff who need it to perform their jobs;
- Incident Response - Report unauthorized disclosures or inspections as prescribed;
- Annual Briefing - Provide annual employee UNAX awareness briefings;
- Monitoring Plan – 3-year on-site review.

Tracking and Disposal of Documents with FTI

A. Proper Tracking
BCS policy *prohibits* the transfer of Federal tax information from KIDS to any other electronic media (e. g., flash drive, CD or DVD disk, laptop, etc.), and the transmission of federal tax information by email or FAX. When staff print federal tax information from KIDS (e.g., screen prints or a case account statement), staff must record the document trail, from creation to disposal.

CSAs may use the attached sample "IRS Tracking and Disposal Log" to track printed federal tax information. The log includes columns to document the following:

- Date Printed
- Staff Name
- IV-D Case # or PIN
- Document Description and Reason Printed
- How Disposed Of
- Date Disposed Of

CSAs must retain Tracking & Disposal logs for five years.

B. Proper Disposal/Destruction
The CSA *must* retain custody of any document containing federal tax information and safeguard the contents until you can properly dispose of the document. Federal tax information may be disposed of by burning, pulping or shredding. The IRS requires shredding in strips 5/16^{ths} of an inch or smaller, and the paper should be inserted in the shredder so that the lines of print are perpendicular to the cutting line.

Federal Tax Information in KIDS

The following printouts and screens may contain IRS information:

- Account History (Path: 05, 14 or 15) -- the C246 Report -- will potentially contain federal tax intercept collections if the worker changes either the Payment History or the Payer Payment History option indicator on the request screen to "Y."
- Federal Tax Offset Collection, source codes FTOC, FTAX and FTXJ; on KIDS Screens FAA and FEB, IV-D Case Account Statement and the Participant Account Statement (Path: 02, 05, 05 & 06 and 05, 09 & 10); they will also be present if you use the F15 print function key on those pages.
- IRS Offsets are also displayed on Screen FIA, List Arrears Certifications (path: 02, 05, 09 and 05, 13) where the Cert Type is "IRS" and there is an amount in the "Offsets" column.
- IRS Offsets are displayed on screens PYE (Inquire Payee Summary 02, 05, 14) and PYR Inquire Payer Summary 02, 05, 15).
- Participant Address, Type "IRS" and/or source codes ***, ***V, ZZZ, or ZZZV; on KIDS Screens AAA and AAB (Path: 02, 01, 04 and 04, 04).
- Participant Name, Types I and J, source codes ZZZ and ZZZV; on KIDS Screens NCA and NCB (Path: 02, 01, 05 and 04, 05).
- CSENet transactions received from other states informing us of a Federal Tax Refund Offset Collection are to be considered federal tax information and must be treated as such.

If you print any of these, you must be aware of and apply safeguard procedures for these documents when they contain federal tax information.

> ***Best Practice Tip:*** Develop agency policy and procedures to prohibit or severely limit the printing of *any* screens or reports containing Federal Tax Information.

Verifying IRS Addresses

Safeguarding standards require that addresses received from the Internal Revenue Service (IRS) be treated as federal tax information and independently verified by another source. However, having the post office confirm that they deliver mail to the person at that address using the Postmaster Verification letter (LO22) does not change the character of the address – the IRS still considers it federal tax information. Before using an address from the IRS (either an IRS type address or source code ***_, ***V, ZZZ_ or ZZZV), child support agencies need to verify the new address by obtaining it from another locate source. Once you obtain the address from a different source, enter it in KIDS as a ***new*** "mail" or "res" address, with an appropriate source code and date.

> ***Best Practice Tip:*** *Never* select or enter the IRS source codes listed above for any information **you** enter in KIDS; if the IRS source codes were not entered by the system, the data did *not* come from the IRS.

Secure Storage of Documents with Federal Tax Information

All federal tax information must be clearly labeled, and handled in such a manner that it does not become misplaced or available to unauthorized personnel. If it is not practical to physically separate files and/or documents containing federal tax information from other case data, the case file must be clearly labeled as containing "federal tax information," and needs to be safeguarded.

The IRS requires that agencies protect federal tax information using Minimum Protection Standards, which call for two barriers, i.e., secured perimeter/locked container; locked perimeter/secured interior; or locked perimeter/secured container. An example of applying this concept is that, if a janitor must have access to a locked file room, that the file cabinets within that room are also locked, preventing the janitor from obtaining access to the federal tax information.

When protecting federal tax information using locked rooms and/or locked containers, the IRS requires the agency to maintain an inventory of all keys or access codes, and the individuals to whom the keys or access codes are issued.

Agencies must limit access to restricted areas, security rooms, and/or locked containers that contain federal tax information, to authorized personnel. If the county or agency issues identification badges to employees, the agency must require that employees wear the identification badge while at work, to identify authorized personnel.

For employees who must enter a restricted area on a regular basis but who are not assigned to that area, the agency may maintain an Authorized Access List, which identifies those individuals. You should review and update an Authorized Access List at least annually.

If other persons must enter an area where federal tax information is kept, the agency must use a Visitor Access Log to document such visits. The attached sample "Visitor Access Log" tracks all IRS-required information. Note that this requirement does not apply to areas within the agency that are designated as publicly accessible.

The Visitor Access Log shall contain the following information:

- Name of visitor and organization represented
- Form of identification used to identify the visitor
- Purpose of visit and person visited
- Date of visit
- Signature of the visitor
- Time of entry and departure

CSAs must retain Visitor Access Logs for five (5) years.

Best Practice Tips:

- If possible, set aside space or use a conference room in a publicly accessible area for conducting participant interviews or appointments.
- Consider making an agency policy to prohibit retention of printed IRS material beyond the end of the workday.

Restrict Access to Those Employees with a Need to Know

BCS and local child support agencies are required to restrict access to federal tax information to employees whose duties or responsibilities require access. No person should be given more federal tax information than is needed to perform his or her duties. For example: when providing KIDS access or documents to a CSA clerk, or staff in a cooperating agency, no federal tax information should be included unless it is needed to perform the required child support duties.

The agency should periodically review which individuals have access to federal tax information and ensure that they still need that information to carry out their job duties. KIDS' users in non-child support agencies (e.g., Economic Support, W-2, Child Welfare, etc.) and other states' child support agencies are not authorized to view federal tax information in KIDS. KIDS blocks the name and address, or blurs the source of payments for these users.

Child support agency staff or attorneys may not disclose federal tax information received from the IRS to the court. You may provide payment records to the court **only** if they do not include source codes for **any** individual payments. If you must use a document that includes payment source codes in court, and that document includes any federal tax refund offset payment, you must redact (black out) the source code for ***all*** payments on the document, not just the federal tax payment(s). From the C246 Account History Report (05, 14 or 15), either the Account Detail Summary or the

Account at-a-Glance options can be used in court because they do not include payment source data. For NCPs who aren't involved as a payer in multiple cases, you can also use either the CSOS Record of Payments for the NCP by Specific Case, or the KIDS Participant Account Statement (Path: 02, 05, 05 or 05, 09).

Incident Response

CSA employees who observe possible improper use or disclosure of IRS information may contact the office of the Special Agent-in-Charge (SAC), Treasury Inspector General for Tax Administration (TIGTA) directly. This individual is located in the Chicago Field Division, 200 W. Adams, Suite 450 Stop 3300 CHI, Chicago, IL 60606, Telephone Number (312) 886-0620, and FAX (312) 886-2397. In the alternative, the CSA employee may contact the BCS Security Officer via KIDPOLCC. All security breaches reported to BCS will be fully investigated.

Annual Briefing on Unauthorized Access (UNAX) Awareness

Local agency managers are required to ensure that all staff know and understand the IRS security and anti-browsing requirements, and have completed the annual awareness briefing requirements. At a minimum, an annual briefing session must be held to ensure that employees are aware of all IRS security requirements. Copies of IRC Section 7213, 7213A and 7431 must be provided to employees annually, and employees must be advised that the unauthorized disclosure of federal tax information could result in civil and criminal penalties as well as the termination of employment. Upon completion of the annual briefing, the employee must read and sign the "Certificate of Need to Know and Annual Unauthorized Access (UNAX) Awareness Briefing," form DWSC–12063, and give it to their supervisor, who should sign it and file in the agency briefing file for that year.

CSAs have three different training resources available, any one of which may be used to conduct the required IRS briefing.

1) Computer-based training programs produced by BCS: "Safeguarding Federal Tax Information" (15 minutes) and "Program Security and Confidentiality" (20 minutes). Both of these CBTs are available on the PTS Learning Center. Upon completion of the Safeguarding Federal Tax Information program, the employee will print the required copies of IRC Sections 7213, 7213A, and 7431, and form DWSC-12063 (see attachments).
2) IRS DVD video "Disclosure Awareness Training for State Child Support Agencies" (30 minutes) this is the 2008 edition. BCS provided copies of this DVD to CSAs in 2009. This video can also be viewed online at: http://www.irsvideos.gov/Governments/Safeguards/DisclosureAwarenessTrainingSCSA
3) IRS videotape which includes "Securing the Future: Giving Hope and Support to America's Children" (20 minutes) and "Stop UNAX In Its Tracks" (15 minutes). Copies of this videotape were provided to CSAs in 2003.

Note: *New employees* should be required to complete the briefing requirement and take **both** of the computer-based training programs under #1 above during the first week of their employment and prior to being granted access to federal tax information.

Agency Briefing Records (Complete by December 31st each year)

The agency must maintain a single file, by year, containing the signed Certificate of Need to Know and Annual Unauthorized Access (UNAX) Awareness Briefing (DWSC-12063) for all staff, to allow for easy inspection by state and/or federal reviewers. These files must be maintained for five (5) years.

CSA Directors must complete, sign and submit the Certification of Compliance with Internal Revenue Service Data Security and Recordkeeping Requirements (DWSC-12065) to the Regional Child Support Administrator.

> ***Best Practice Tip:*** Tie the scheduling of your annual briefing activities to another annual agency event or milestone, or create an Outlook Calendar task or event to give you an automatic reminder.

Monitoring Plan

IRS Safeguarding rules require regular monitoring of agencies that receive federal tax data. The Department's Child Support Regional Coordinators conduct on-site safeguard reviews to evaluate the security measures the agency has taken to ensure the confidentiality and adequate protection of FTI provided by the IRS. Agencies are required to provide verification of all employee's participation in annual awareness briefing; the *Certification of Need to Know and Annual Unauthorized Access (UNAX) Awareness Briefing* documents the successful completion of on-line training. Agencies must also provide the completed Certificate of Compliance with IRS Data Security (DWSC-12065). The reviews shall be conducted a minimum of once every three years.

Thank you for your continued attention to these important requirements.

Resources:

IRS Publication 1075 Tax Information Security Guidelines for Federal, State and Local Agencies